

SYSTEM FOR DISTRIBUTING INFORMATION TO VEHICLE AND METHOD FOR THE SAME

Publication number: JP2002333989 (A)

Publication date: 2002-11-22

Inventor(s): TOMITA HITOSHI; KITAZAWA SHUJI

Applicant(s): HITACHI LTD

Classification:

- international: G06F12/14; G06F11/00; G06F21/22; G06F21/24; G06F12/14; G06F11/00; G06F21/00; G06F21/22; (IPC1-7): G06F11/00; G06F12/14

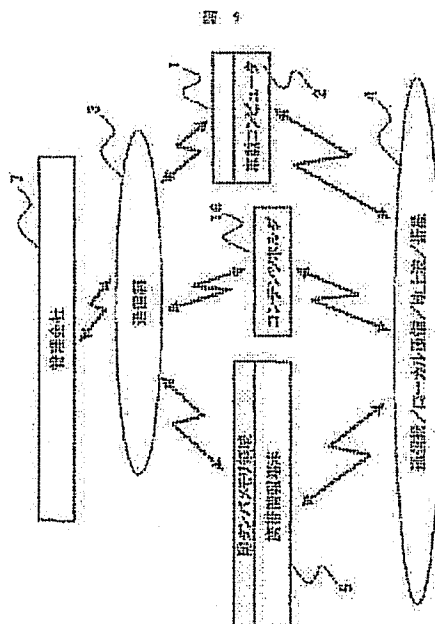
- European:

Application number: JP20010139436 20010510

Priority number(s): JP20010139436 20010510

Abstract of JP 2002333989 (A)

PROBLEM TO BE SOLVED: To provide an information distributing system and method capable of preventing any inconvenience from being generated in vehicle control at the time of inputting contents to be distributed to a vehicle. **SOLUTION:** A computer 8 of a management company 7 receives a contents and virus check authentication request signal transmitted from a vehicle 1 or receives the contents name, and diagnoses the transmitted contents or the contents received from a contents providing company by referring to a virus data base and a vaccine data base by a server for analyzing contents, and at the time of judging that the contents are not infected by any virus, or at the time of removing the virus from the contents, transmits the contents added with an electronic key to the vehicle 1, and inputs the contents to a computer 2 of the vehicle 1.



Data supplied from the esp@cenet database — Worldwide

(11)特許出願公開番号

特開2002-333989

(P2002-333989A)

(43)公開日 平成14年11月22日(2002.11.22)

(51) Int.Cl.⁷

識別記号

FI

デーコート^a(参考)

G 0 6 F 11/00

C O 6 F 12/14

320F 5B01.7

12/14

320

9/06

660N 5B076

審査請求 未請求 請求項の数7 OL (全 15 頁)

(21)出願番号 特願2001-139436(P2001-139436)

(22) 出願日 平成13年5月10日(2001.5.10)

(71)出願人 000003108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72)発明者 富田 仁志

東京都千代田区神田駿河台四丁目6番地

株式会社日立製作所システム事業部内

(72) 発明者 北沢 修司

東京都千代田区神田駿河台四丁目6番地

株式会社日立製作所システム事業部内

(74) 代理人 100075096

弁理士 作田 康夫

Fターム(参考) 5B017 AA06 BA09 BB09 BB10 CA16

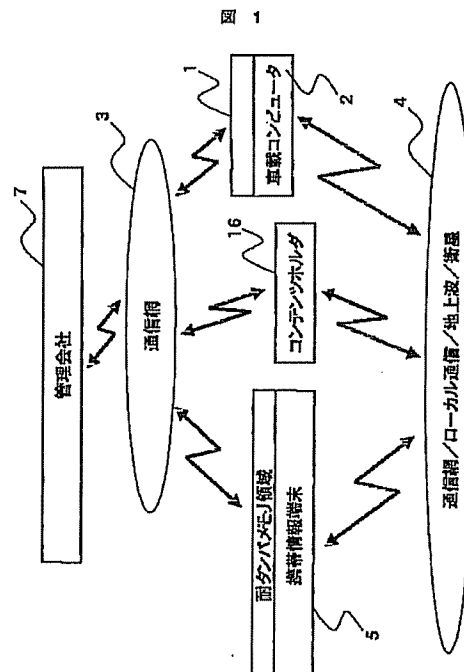
5B076 FD08

(54) 【発明の名称】 車両への情報配信システム及びその方法

(57) 【要約】

【課題】車両に配信されるコンテンツを入力する場合に車両制御に不都合が生じるのを防止できる車両への情報配信システム及びその方法を提供する。

【解決手段】管理会社7のコンピュータ8が車両1から送信されたコンテンツ及びウイルスチェック認証要求信号を受信、もしくはコンテンツ名を受信し、送信されたコンテンツもしくはコンテンツ提供会社から受信したコンテンツを、コンテンツ解析用のサーバによりウイルスデータベース、ワクチンデータベースを参照して診断してウイルスに感染されていないと判断した、もしくはコンテンツからウイルスを除去できた場合は、コンテンツに電子キーを付して車両1に送信し、車両1のコンピュータ2に入力する。



【特許請求の範囲】

【請求項1】ウィルスデータベースと、ワクチンデータベースと、コンテンツ解析用のサーバとを備え、車両からのコンテンツとウィルスチェック認証要求信号を受信して前記コンテンツ解析用のサーバが前記ウィルスデータベース、ワクチンデータベースを参照して前記コンテンツを診断してウィルスに感染されていないと判断した、もしくはコンテンツからウィルスを除去できた場合は、該コンテンツに電子キーを付して前記車両に送信することを特徴とする車両への情報配信システム。

【請求項2】ウィルスデータベースと、ワクチンデータベースと、コンテンツ解析用のサーバとを備え、車両からの希望するコンテンツ名を受信して該コンテンツを入手するとともに前記コンテンツ解析用のサーバが前記ウィルスデータベース、ワクチンデータベースを参照して前記コンテンツを診断してウィルスに感染されていないと判断した、もしくはコンテンツからウィルスを除去できた場合は、該コンテンツに電子キーを付して前記車両に送信することを特徴とする車両への情報配信システム。

【請求項3】受信したコンテンツを記憶する記憶部と、ウィルスチェック認証要求信号を作成する制御部と、前記コンテンツとウィルスチェック認証要求信号を管理会社に送信する通信装置とを備えた車両であって、前記管理会社から電子キーを付されたコンテンツを前記通信装置により受信した場合、前記制御部により前記電子キーとコンテンツを車両のコンピュータに送信することを特徴とする車両への情報配信システム。

【請求項4】希望するコンテンツ名を作成する制御部と、該コンテンツ名を管理会社に送信する通信装置とを備えた車両であって、前記管理会社から電子キーを付されたコンテンツを前記通信装置により受信した場合、前記制御部により前記電子キーとコンテンツを車両のコンピュータに送信することを特徴とする車両への情報配信システム。

【請求項5】車の設定情報を記憶する記憶部と、該車の設定情報について運転者の変更したい要望を入力する入力部と、該入力部で入力された前記変更したい要望を管理会社に送信する通信装置を備え、管理会社から電子キーを付された変更された車の設定情報を前記通信装置により受信して該電子キーが予め記録されている電子キーと照合することを条件に前記変更された車の設定情報を前記記憶部に記憶することを特徴とする車両への情報配信システム。

【請求項6】管理会社のコンピュータが車両から送信されたコンテンツ及びウィルスチェック認証要求信号を受信、もしくはコンテンツ名を受信し、前記送信されたコンテンツもしくはコンテンツ提供会社から受信したコンテンツを、コンテンツ解析用のサーバによりウィルスデータベース、ワクチンデータベースを参照して診断して

ウィルスに感染されていないと判断した、もしくはコンテンツからウィルスを除去できた場合は、該コンテンツに電子キーを付して前記車両に送信し、車両のコンピュータに入力することを特徴とする車両への情報配信方法。

【請求項7】車両から受信したコンテンツ及び作成したウィルスチェック認証要求信号、もしくは希望するコンテンツ名を管理会社に送信し、該管理会社から電子キーを付されたコンテンツを受信した場合、前記電子キーとコンテンツを車両のコンピュータに送信することを特徴とする車両への情報配信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、例えば自動車に搭載されているコンピュータにコンテンツ情報を安全に提供するのに好適な車両への情報配信システム及びその方法に関する。

【0002】

【従来の技術】従来の技術としては、例えば特開平11-122162号公報に記載のように、搭乗時にIDカードやその他の入力手段からの入力により搭乗者全員の個人認証を実施し、その個人認証情報により受け取ったメッセージの配信レベルで配信先を決定するとともに、車両の走行状態や車両環境の認識により情報配信が可能な状態かどうかを決定して情報を配信する車両内情報配信システムがある。又、特開平11-274999号公報に記載のように、固定局と複数の移動体間の暗号通信に複数のバージョンの共通鍵を使用するようにし、移動体は通信要求時に自局の鍵バージョンを送信し、固定局は受信した鍵バージョンの通常鍵が有効にサポートされているかを判定して有効な場合には当該バージョンと鍵用途(通常)を応答、無効な場合は当該鍵バージョンと鍵用途(緊急)を応答するようにした移動体通信システムがある。

【0003】

【発明が解決しようとする課題】特開平11-122162号公報に記載の車両内情報配信システムは、搭乗者の配信レベル、車両の走行状態や車両環境の認識により車両が受信した情報を安全に配信するものであるが、この従来の技術では、車両が受信した情報がコンピュータウィルスに感染している、あるいは既にコンピュータに入力されている情報を改ざんするものであった場合を想定したものではないので、車両の制御プログラムが破壊され、重大な事故に繋がることを防止する点についての配慮がなされていない。又、特開平11-274999号公報に記載の移動体通信システムは、通信のセキュリティの向上となるものではあるが、この従来の技術も受信した情報がコンピュータウィルスに感染していた場合、車両の制御プログラムが破壊され、重大な事故に繋がることを防止する点の配慮がなされていない。

【0004】本発明の第1の目的は、車両に配信されるコンテンツを入力する場合に車両制御に不都合が生じるのを防止できる車両への情報配信システム及びその方法を提供することにある。

【0005】本発明の第2の目的は、ウィルスに感染されたコンテンツが車両のコンピュータに侵入するのを防止できる車両への情報配信システム及びその方法を提供することにある。

【0006】本発明の第3の目的は、車の設定値情報を変更する場合に改ざんを防止できる車両への情報配信システム及びその方法を提供することにある。

【0007】

【課題を解決するための手段】上記第1、第2の目的を達成するために、本発明の車両への情報配信システムは、車両からのコンテンツとウィルスチェック認証要求信号を受信してコンテンツ解析用のサーバがウィルスデータベース、ワクチンデータベースを参照して前記コンテンツを診断してウィルスに感染されていないと判断した、もしくはコンテンツからウィルスを除去できた場合は、該コンテンツに電子キーを付して前記車両に送信することを特徴とする。

【0008】又、車両からの希望するコンテンツ名を受信して該コンテンツを入手するとともにコンテンツ解析用のサーバがウィルスデータベース、ワクチンデータベースを参照して前記コンテンツを診断してウィルスに感染されていないと判断した、もしくはコンテンツからウィルスを除去できた場合は、該コンテンツに電子キーを付して前記車両に送信することを特徴とする。

【0009】又、コンテンツとウィルスチェック認証要求信号を管理会社に送信する通信装置とを備えた車両であって、前記管理会社から電子キーを付されたコンテンツを前記通信装置により受信した場合、前記制御部により前記電子キーとコンテンツを車両のコンピュータに送信することを特徴とする。

【0010】又、希望するコンテンツ名を管理会社に送信する通信装置とを備えた車両であって、前記管理会社から電子キーを付されたコンテンツを前記通信装置により受信した場合、制御部により前記電子キーとコンテンツを車両のコンピュータに送信することを特徴とする。

【0011】又、車両への情報配信方法は、管理会社のコンピュータが車両から送信されたコンテンツ及びウィルスチェック認証要求信号を受信、もしくはコンテンツ名を受信し、前記送信されたコンテンツもしくはコンテンツ提供会社から受信したコンテンツを、コンテンツ解析用のサーバによりウィルスデータベース、ワクチンデータベースを参照して診断してウィルスに感染されていないと判断した、もしくはコンテンツからウィルスを除去できた場合は、該コンテンツに電子キーを付して前記車両に送信し、車両のコンピュータに入力することを特徴とする。

【0012】又、車両から受信したコンテンツ及び作成したウィルスチェック認証要求信号、もしくは希望するコンテンツ名を管理会社に送信し、該管理会社から電子キーを付されたコンテンツを受信した場合、前記電子キーとコンテンツを車両のコンピュータに送信することを特徴とする。

【0013】上記第3の目的を達成するために、本発明の車両への情報配信システムは、車の設定情報を記憶する記憶部と、該車の設定情報について運転者の変更したい要望を入力する入力部と、該入力部で入力された前記変更したい要望を管理会社に送信する通信装置を備え、管理会社から電子キーを付された変更された車の設定情報を前記通信装置により受信して該電子キーが予め記録されている電子キーと照合することを条件に前記変更された車の設定情報を前記記憶部に記憶することを特徴とする。

【0014】

【発明の実施の形態】本発明の一実施例を図1から図4により説明する。車両への情報配信システムとして、以下では自動車为例にとり説明するが、電車等の移動体に適用することができる。図1、図2に示すように、本実施例の車両への情報配信システムは、自動車1（車両1ともいう）に搭載され自動車の走行制御等に使用されるコンピュータ2、コンピュータ2と双方向のブロードバンドの通信網3もしくはローカル通信、地上波、衛星通信等の通信回線4で接続されたカーナビゲーション装置5a、PDA(Personal Digital Assistantsの略)などの携帯端末5b、携帯電話5cもしくは携帯パソコン5dなどの携帯情報端末5、携帯情報端末5と双方向のブロードバンドの通信網3で接続された管理会社7のコンピュータ8で構成される。コンピュータ8は、図示しない外部の最新のコンピュータウィルス情報とワクチンプログラム情報の提供会社のコンピュータ、自動車に関する詳細情報の提供会社のコンピュータ、コンテンツの提供会社のコンピュータと通信網3を介して接続されている。コンピュータ2、携帯情報端末5は、通信網3もしくは通信回線4でコンテンツの提供会社であるコンテンツホルダ16と接続されている。

【0015】管理会社7のコンピュータ8は、図3に示すように、コンテンツ解析用のサーバ9、認証用のサーバ10と課金用のサーバ11、課金データベース12、証明書データベース13、ウィルスデータベース、ワクチンデータベース、安全設定値データベースなどで構成される情報データベース14、それらを接続するネットワーク15で構成されている。情報データベース14には、外部の提供会社から受信して蓄積したコンピュータウィルス情報、自動車の安全設定に関する車の設定値情報が記録されている。

【0016】携帯情報端末5は、図4に示すように、通信装置20に接続された通信インターフェイス21、通

信インターフェイス21にバス28を介して接続されたCPU22, RAM/ROMの記憶部23, フラッシュカードインターフェース24, 入力部25, 出力部26, 制御部27で構成される。携帯情報端末5にはフラッシュカード16の挿入口が設けられ、フラッシュカードインターフェース24部にフラッシュカード16を装着した状態で使用する。フラッシュカード16には、車の設定情報、アプリケーションプログラム、各種コンテンツを記憶する通常メモリ領域16aと、外部からの不正な改ざんを防止するための耐タンパ領域16bが設けられている。RAM/ROMの記憶部23に通常メモリ領域の他に耐タンパ領域を設けることもでき、この場合は、フラッシュカード及びフラッシュカードインターフェイスを省略することができる。

【0017】コンピュータ2は、図5に示すように、通信装置30に接続された通信インターフェイス31, 通信インターフェイス31のすぐ後に設けられたバッファ領域40, バッファ領域40とバス41を介して接続されたCPU32, RAM/ROMの記憶部33, 認証書チェック部34, 入力部35, 出力部36, 制御部37, 大容量ストレージ38, 各種のセンサ39で構成される。

【0018】次に、このように構成された車両情報提供システムの動作について説明する。以下、この種の動作をタイプ1という。図6, 図8に示すように、搭乗者が、ステップ101で携帯情報端末5もしくはコンピュータ2の入力部35を操作して入手を希望するコンテンツ名を入力もしくは選択して送信すると、コンテンツホルダ16は希望したコンテンツを携帯情報端末5に送信する。コンテンツを受信した携帯情報端末5では、受信したコンテンツをコンピュータ2に送信することなく、携帯情報端末5の記憶部23に記憶する。携帯情報端末5の制御部27では、図6, 図8に示すように、管理会社7のコンピュータ8に送信するウィルスチェック認証要求信号を作成する。又、ウィルスチェックを行うコンテンツを特定するためにコンテンツID, 送信した車両を特定するための車両IDを作成もしくは予め定義されている車両IDを用いて、ステップ102で要求信号, コンテンツID, 車両ID及びコンテンツを通信インターフェイス21, 通信装置20を介して管理会社7のコンピュータ8に送信する。

【0019】図9に示すステップ121で要求信号, コンテンツID, 車両ID及びコンテンツを受信したコンピュータ8では、ステップ122でコンテンツ解析用のサーバ9により受信したコンテンツを解析する。すなわち、ウィルスデータベースを参照してウィルス診断プログラムにより配信されたコンテンツがウィルスに感染しているか否かを診断する。ウィルスに感染していないと判断された場合は、ステップ123～125で証明書データベース13を参照して認証用のサーバ10にて予め

個々の自動車1毎に発行されている電子キーをコンテンツIDに付して携帯情報端末5に送信する。ステップ126でウィルスに感染していると判断された場合は、ステップ127, 128でワクチンデータベースを参照してコンテンツ解析用のサーバ9でコンテンツからウィルスを除去する。コンテンツからウィルスを除去できた場合は、ステップ123～125で作成したコンテンツに電子キーを付して携帯情報端末5に送信する。コンテンツ解析用のサーバ9でウィルスを除去できない場合、又は携帯情報端末5からウィルスを除去してほしいとの要望がなかった場合は、ステップ129, 125でコンテンツIDにウィルスに感染している情報を付して携帯情報端末5に返信する。

【0020】図8に示すステップ103でコンテンツID, 電子キー又はコンテンツがウィルスに感染している情報、コンテンツを受信した携帯情報端末5では、ステップ104で電子キーを受信したことにより、ステップ106で耐タンパ領域に電子キーを格納する。図10に示すステップ131で携帯情報端末5は、コンテンツの送信要求信号と電子キーをコンピュータ2に送信する。ステップ132で証明書である電子キーを受信したコンピュータ2は、ステップ133で受信した電子キーと予め登録されている電子キーとの照合を行い、照合された場合は、ステップ135で携帯情報端末5にウィルスに感染していないコンテンツを自動車1のコンピュータ2に送信することを要求する信号を送る。コンテンツを受信したコンピュータ2では、そのコンテンツを記憶部33に記録する。ステップ133で受信した電子キーと予め登録されている電子キーとの照合を行い、照合されなかった場合は、コンテンツの送信要求信号は作成されず、ステップ137で携帯情報端末5に不許可通知を行い表示する。この表示を見て搭乗者は、管理会社7に確認する等の措置をとることができる。

【0021】電子キーが付されていないウィルスに感染したコンテンツを受信した場合は、携帯情報端末5は、該当するコンテンツ名又はコンテンツID, ウィルスに感染されていることを表示する。搭乗者は、その表示を見て、コンテンツを消去する等の処理を行う。

【0022】このように、送信されたコンテンツがウィルスに感染されているか否かを管理会社でチェックした後、ウィルスに感染されていないコンテンツをコンピュータに入力するので、車両の制御プログラムが破壊され、重大な事故に繋がることを防止することができる。一般に車両側では、最新のウィルス情報に反映させて対策を講じるのは、個人では実現しにくい、管理会社に入手したコンテンツを送信して診断することにより、最新のウィルスに対しても対策することができる。又、コンテンツがウィルスに感染している場合でも、管理会社側でウィルスを削除することができ、金を払って入手したコンテンツを無駄にすることが少なくなるという効果

がある。又、車両に予め設定されている電子キーで照合された場合に、車両のコンピュータがコンテンツを受信するようにしているので、管理会社から送信される以外の情報を遮断することができ、管理会社からの誤った送信を受信するのを防止できる。

【0023】次に車の設定値情報について説明する。自動車の購入者及び通常運転する人を登録しておく、その人の年齢、性別、運転歴、体力的な要件等により、ハンドルの重さ加減、アクセルの重さ加減、ブレーキを踏む時の重さ加減、速度の上限値、変速するタイミング、加速性等についての制御定数を車の設定値情報として予めコンピュータ2の記憶部33に記録しておく。運転者が設定されている車の設定値情報で自動車を運転した結果、その運転者の好みに合わせて例えばハンドルの重さ加減を変更したい場合には、コンピュータ2の入力部35又は携帯情報端末5を操作して、運転者の変更したい要望を入力し、通信インターフェース21、通信装置20を介して管理会社7に送信する。この情報を受信した管理会社7のコンピュータ8は、安全設定値データベースを参照してコンテンツ解析用のサーバ9により車の設定値情報を更新する。この更新される車の設定値情報は、コンテンツ解析用のサーバでウィルス感染のチェックがなされており、ウィルス感染のないデータとなっている。更新された車の設定値情報には、電子キーが付されて自動車1のコンピュータ2に送信される。電子キーが付された車の設定値情報を受信したコンピュータ2では、予め登録されている電子キーと照合を行い、キーが合うことを条件に車の設定値情報を記憶部33に記録する。

【0024】このように、運転者に対応した車の制御定数で車両を運転できるので、その人に適した運転が行える。又、運転する人の嗜好に応じて車の設定値情報を変更する際に、管理会社に蓄積されている新しい情報によって変更できるので、より適した車の運転が行える。又、車両に予め設定されている電子キーで照合された場合に、車両のコンピュータが車の設定値情報を受信するようにしているので、管理会社から送信される以外の情報を遮断することができ、管理会社からの誤った送信を受信するのを防止できる。

【0025】図7は、本実施例の変形例を示す流れ図であり、この例では、携帯情報端末5もしくはコンピュータ2は、コンテンツホルダ16から直接コンテンツを受信するのではなく、希望するコンテンツがあると、希望するコンテンツを管理会社7から送信してもらうようにしている。以下、これをタイプ2という。図8に示すステップ109で、搭乗者が、携帯情報端末5もしくはコンピュータ2の入力部35を操作して入手を希望するコンテンツ名を入力もしくは選択して車両を特定するための車両IDとともに管理会社7に送信すると、管理会社7は、図9のステップ121でコンテンツ提供会社から

希望するコンテンツを受信する。コンテンツを受信したコンピュータ2では、ステップ122でコンテンツ解析用のサーバ9により受信したコンテンツを診断する。ウィルスに感染していないと判断された場合は、ステップ123～125で証明書データベース13を参照して認証用のサーバ10にて予め個々の自動車1毎に発行されている電子キーをコンテンツIDに付して携帯情報端末5に送信する。ステップ126でウィルスに感染していると判断された場合は、ステップ127、128でコンテンツ解析用のサーバ9でコンテンツからウィルスを除去する。コンテンツからウィルスを除去できた場合は、ステップ123～125で作成したコンテンツに電子キーを付して携帯情報端末5に送信する。コンテンツ解析用のサーバ9でウィルスを除去できない場合は、ステップ129、125で希望するコンテンツがウィルスに感染している情報を付して携帯情報端末5に返信する。

【0026】図8に示すステップ110で認証済みのコンテンツを受信した携帯情報端末5では、ステップ105で耐タンパ領域に電子キーを格納する。図10に示すステップ131で携帯情報端末5は、コンテンツの送信要求信号と電子キーをコンピュータ2に送信する。ステップ132で証明書である電子キーを受信したコンピュータ2は、ステップ133で受信した電子キーと予め登録されている電子キーとの照合を行い、照合された場合は、ステップ135で携帯情報端末5にコンテンツを自動車1のコンピュータ2に送信することを要求する信号を送る。コンテンツを受信したコンピュータ2では、そのコンテンツを記憶部33に記録する。ステップ133で受信した電子キーと予め登録されている電子キーとの照合を行い、照合されなかった場合は、コンテンツの送信要求信号は作成されず、ステップ137で携帯情報端末5に不許可通知を行い、表示する。この表示を見て搭乗者は、管理会社7に確認する等の措置をとることができる。

【0027】この例では、希望するコンテンツを管理会社でチェックした後、ウィルスに感染されていないコンテンツをコンピュータに入力するので、ウィルスに感染したコンテンツを車両側に受信することがなくなり、車両の制御プログラムが破壊され、重大な事故に繋がることをより防止することができる。又、ウィルスに感染しているコンテンツを予め管理会社側でチェックでき、金を払って入手したコンテンツを無駄にすることが少なくなるという効果がある。又、車両に予め設定されている電子キーで照合された場合に、車両のコンピュータがコンテンツを受信するようにしているので、管理会社から送信される以外の情報を遮断することができ、管理会社からの誤った送信を受信するのを防止できる。

【0028】図11から図14に示す例は、携帯情報端末5を用いなく、コンピュータ2のバッファ領域40を使用してコンテンツの入手を行うものであり、図11、

図12に示す例は、コンピュータ2の入力部を操作して、コンテンツをコンテンツホルダ16から入手する場合（以下、タイプ3という）、図13、図14に示す例は、コンピュータ2の入力部を操作して、コンテンツを管理会社7から入手する場合（以下、タイプ4という）を示している。

【0029】図11、図12に示す例では、搭乗者が、ステップ151でコンピュータ2の入力部35を操作して入手を希望するコンテンツ名を入力もしくは選択して送信すると、コンテンツホルダ16は希望したコンテンツを携帯情報端末5に送信する。コンテンツを受信したコンピュータ2では、受信したコンテンツをバッファ領域40に記憶する。制御部37では、管理会社7のコンピュータ8に送信するウィルスチェック認証要求信号を作成する。又、ウィルスチェックを行うコンテンツを特定するためにコンテンツID、送信した車両を特定するための車両IDを作成もしくは予め定義されている車両IDを用いて、ステップ152、153で要求信号、コンテンツID、車両ID及びコンテンツを通信インターフェイス31、通信装置30を介して管理会社7のコンピュータ8に送信する。

【0030】要求信号、コンテンツID、車両ID及びコンテンツを受信したコンピュータ2では、上述したようにコンテンツがウィルスに感染しているか否かを診断して、ウィルスに感染していないと判断された場合は、電子キーをコンテンツIDに付してコンピュータ2に送信する。ウィルスに感染していると判断された場合は、コンテンツからウィルスを除去し、作成したコンテンツに電子キーを付してコンピュータ2に送信する。ウィルスを除去できない場合、又はコンピュータ2からウィルスを除去してほしいとの要望がなかった場合は、コンテンツIDにウィルスに感染している情報を付してコンピュータ2に返信する。

【0031】図12に示すステップ154でコンテンツID、電子キー又はコンテンツがウィルスに感染している情報、コンテンツを受信したコンピュータ2では、ステップ155で電子キーを受信したことにより、ステップ156で受信した電子キーと予め登録されている電子キーとの照合を行い、照合された場合は、ステップ137でコンテンツをコンピュータ2の記憶部33に記録する。ステップ133で受信した電子キーと予め登録されている電子キーとの照合を行い、照合されなかった場合は、ステップ159で管理会社7に不許可通知を行い、表示する。この表示を見て搭乗者は、管理会社7に確認する等の措置をとることができる。

【0032】この例では、コンピュータ2にバッファ領域を設けてコンテンツがウィルスに感染されているか否かを管理会社でチェックした後、ウィルスに感染していないコンテンツをコンピュータに入力するので、携帯情報端末を用いなくても、車両の制御プログラムが破壊

され、重大な事故に繋がることを防止することができる。又、車両に予め設定されている電子キーで照合された場合に、車両のコンピュータがコンテンツを受信するようにしているので、管理会社から送信される以外の情報を遮断することができ、管理会社からの誤った送信を受信するのを防止できる。

【0033】図13、図14に示す例では、図14に示すステップ161で、搭乗者が、コンピュータ2の入力部35を操作して入手を希望するコンテンツ名を入力もしくは選択して車両を特定するための車両IDとともに管理会社7に送信すると、管理会社7では、上述したように、コンテンツ提供会社から希望するコンテンツを受信し、コンテンツを診断する。ウィルスに感染していないと判断された場合は、電子キーをコンテンツに付してコンピュータ2に送信する。ウィルスに感染していると判断された場合は、コンテンツからウィルスを除去し、コンテンツに電子キーを付してコンピュータ2に送信する。ウィルスを除去できない場合は、希望するコンテンツがウィルスに感染している情報を付してコンピュータ2に返信する。

【0034】図14に示すステップ162で認証済みのコンテンツを受信したコンピュータ2では、バッファ領域に認証済みのコンテンツを格納する。証明書である電子キーを受信したコンピュータ2は、ステップ163で受信した電子キーと予め登録されている電子キーとの照合を行い、照合された場合は、ステップ164でコンテンツを記憶部33に記録する。照合されなかった場合は、ステップ166で管理会社7に不許可通知を行い、表示する。この表示を見て搭乗者は、管理会社7に確認する等の措置をとることができる。

【0035】この例では、携帯情報端末を用いることなく、希望するコンテンツを管理会社でチェックした後、ウィルスに感染されていないコンテンツをコンピュータに入力するので、ウィルスに感染したコンテンツを車両側に受信することがなくなり、車両の制御プログラムが破壊され、重大な事故に繋がることをより防止することができる。又、ウィルスに感染しているコンテンツを予め管理会社側でチェックでき、金を払って入手したコンテンツを無駄にすることが少なくなるという効果がある。又、車両に予め設定されている電子キーで照合された場合に、車両のコンピュータがコンテンツを受信するようにしているので、管理会社から送信される以外の情報を遮断することができ、管理会社からの誤った送信を受信するのを防止できる。

【0036】

【発明の効果】本発明によれば、ウィルスに感染されていないコンテンツをコンピュータに入力するので、車両の制御プログラムが破壊され、重大な事故に繋がることを防止することができる。

【図面の簡単な説明】

【図1】本発明の一実施例である車両への情報配信システムの構成図である。

【図2】本実施例の構成図である。

【図3】管理会社のコンピュータの構成図である。

【図4】携帯情報端末の構成図である。

【図5】車両のコンピュータの構成図である。

【図6】情報の流れを示す図である。

【図7】情報の流れを示す図である。

【図8】携帯情報端末での処理の流れ図である。

【図9】管理会社のコンピュータでの処理の流れ図である。

【図10】車両のコンピュータでの処理の流れ図である。

【図11】情報の流れを示す図である。

【図12】車両のコンピュータでの処理の流れ図である。

る。

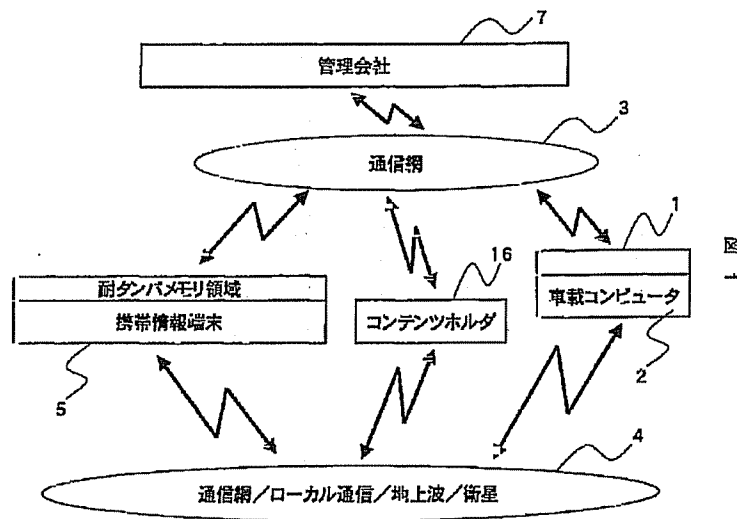
【図13】情報の流れを示す図である。

【図14】車両のコンピュータでの処理の流れ図である。

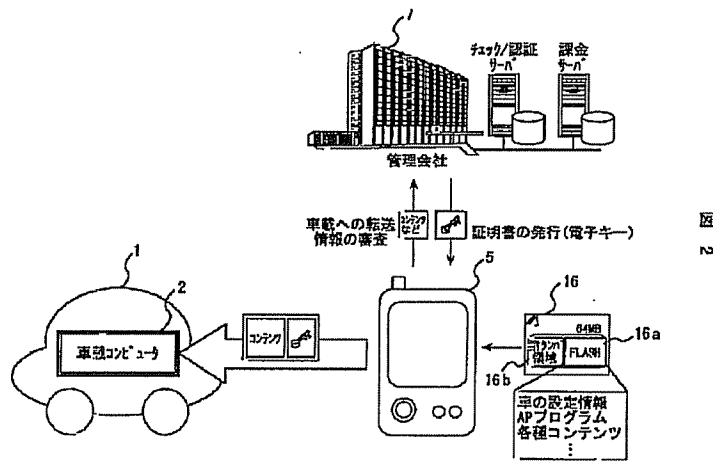
【符号の説明】

1…自動車、2, 8…コンピュータ、3, 6…通信網、4…ローカル通信、5…携帯情報端末、7…管理会社、9, 10, 11…サーバ、12…課金データベース、13…証明書データベース、14…情報データベース、16…フラッシュカード、20, 30…通信装置、21, 31…通信インターフェイス、22, 32…CPU、23, 33…記憶部、24…フラッシュカードインターフェイス、25, 35…入力部、26, 36…出力部、27, 37…制御部、38…大容量ストレージ、39…センサ。

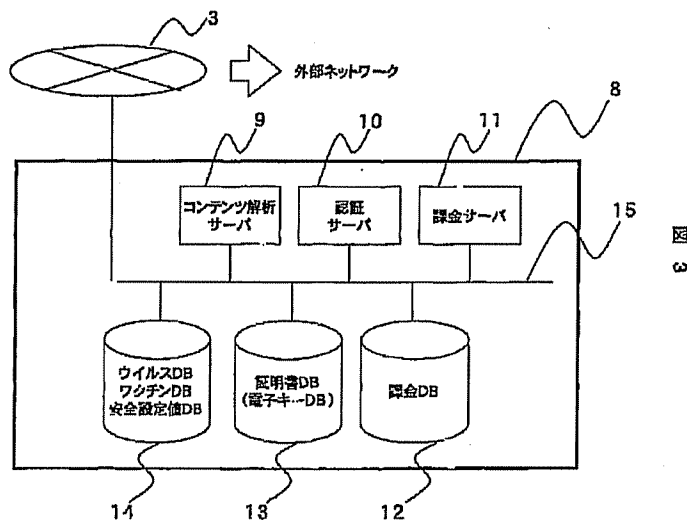
【図1】



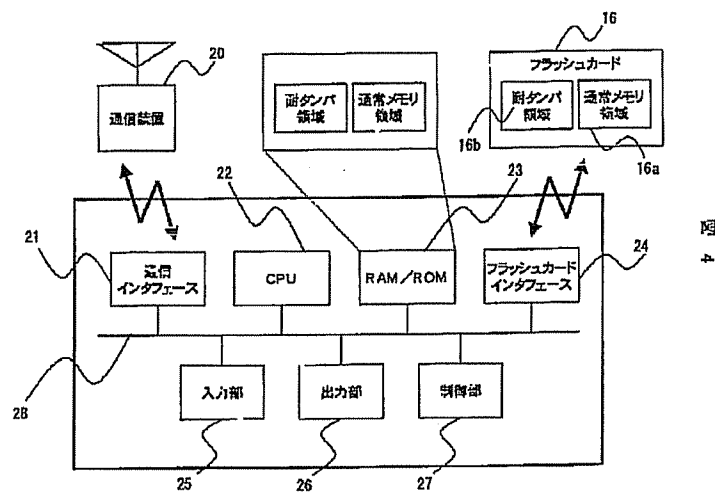
【図2】



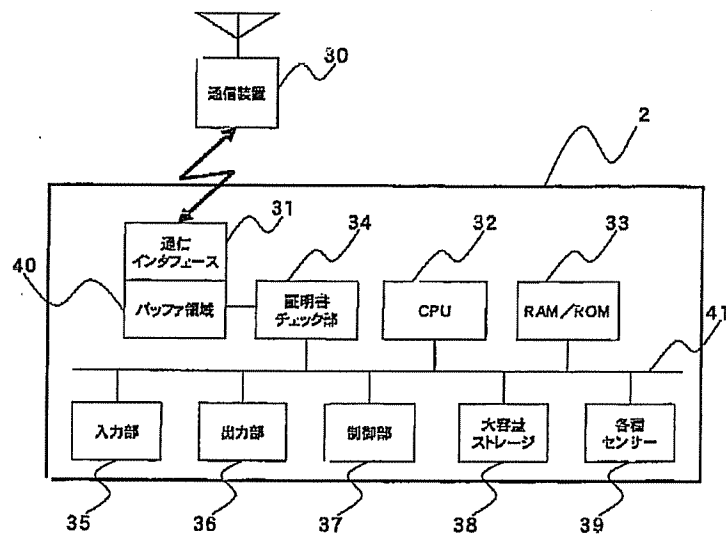
【図3】



【図4】



【図5】



【図6】

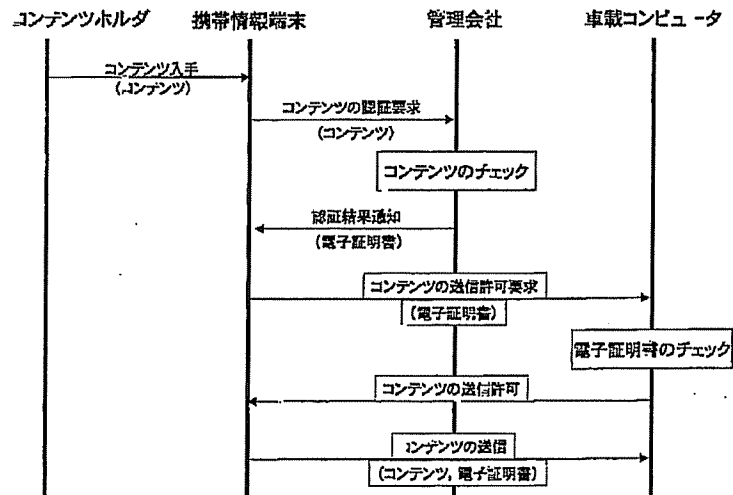


図 6

【図7】

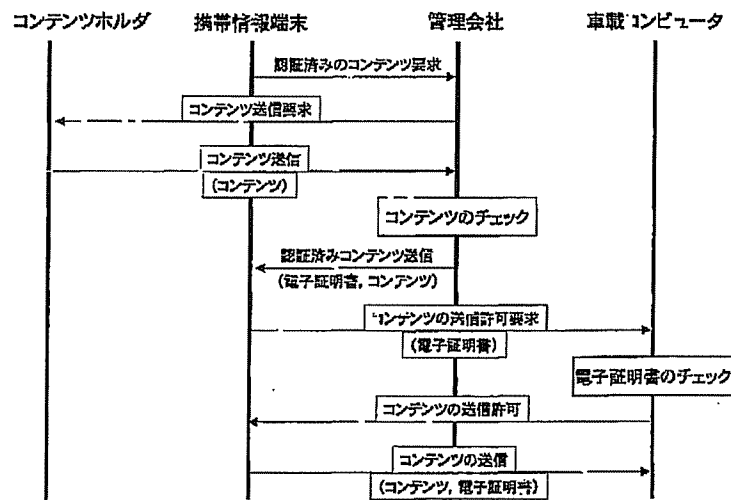
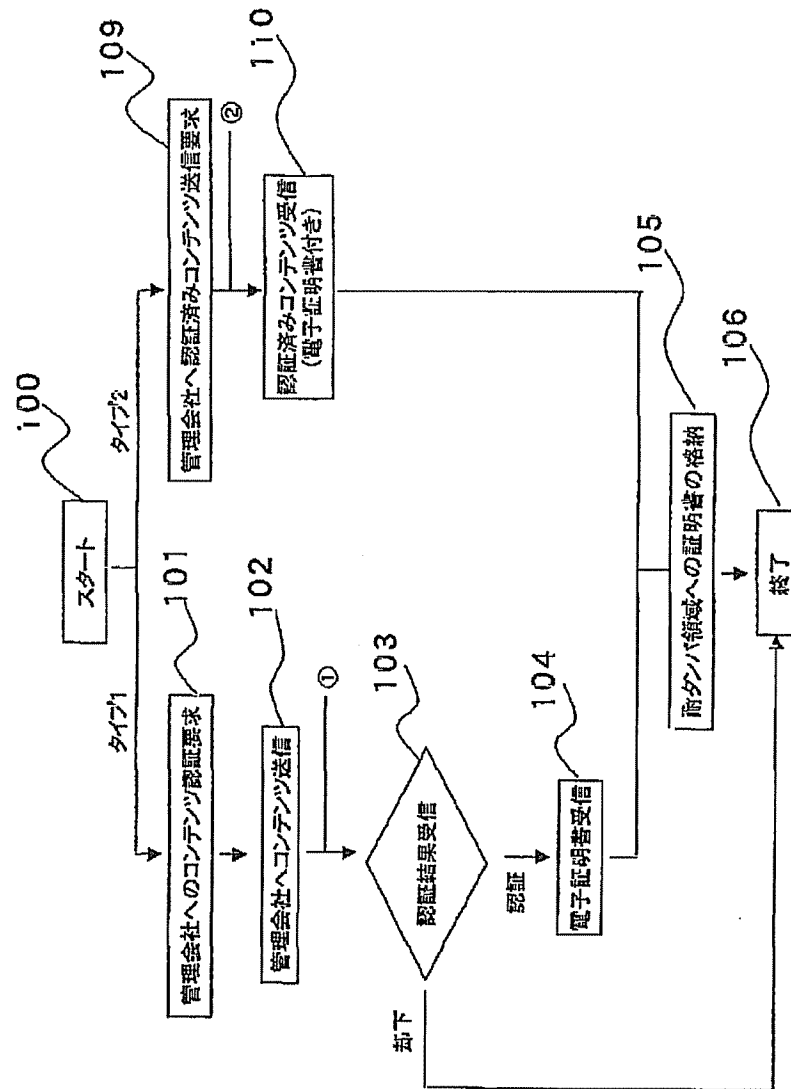


図 7

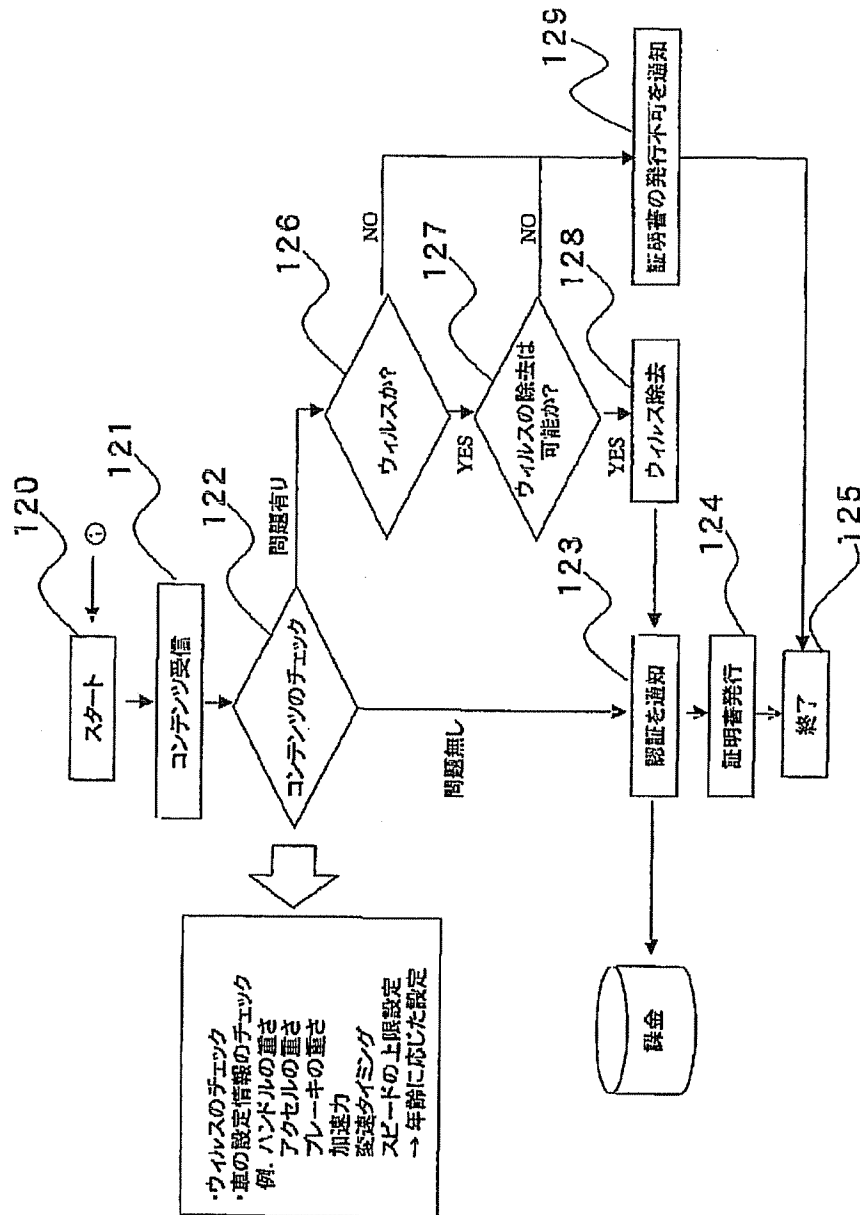
【図8】

図 8



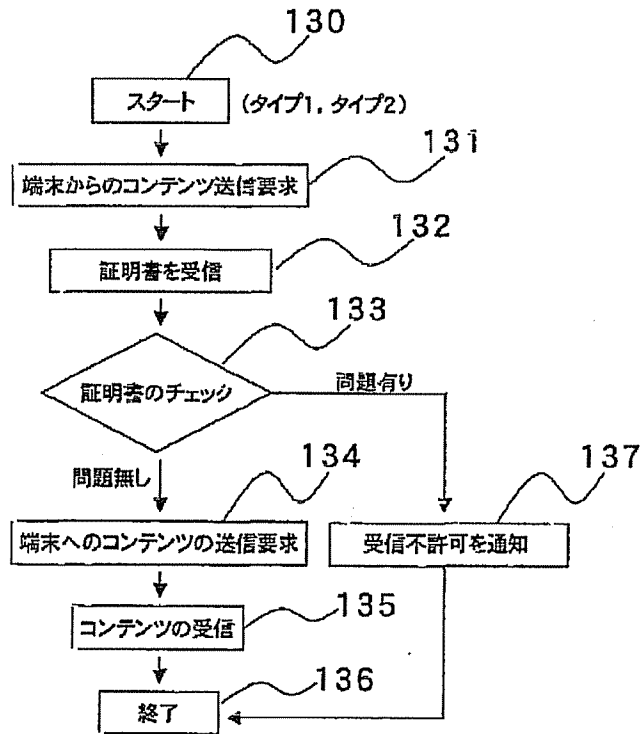
【図9】

図 9

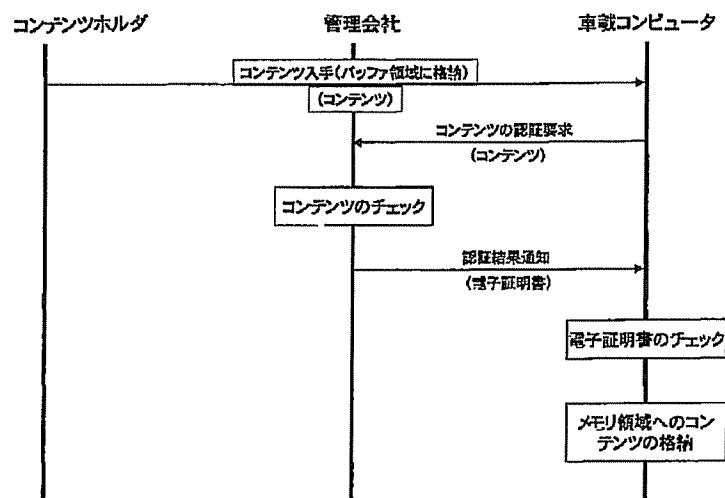


【図10】

図 10



【図11】



【図12】

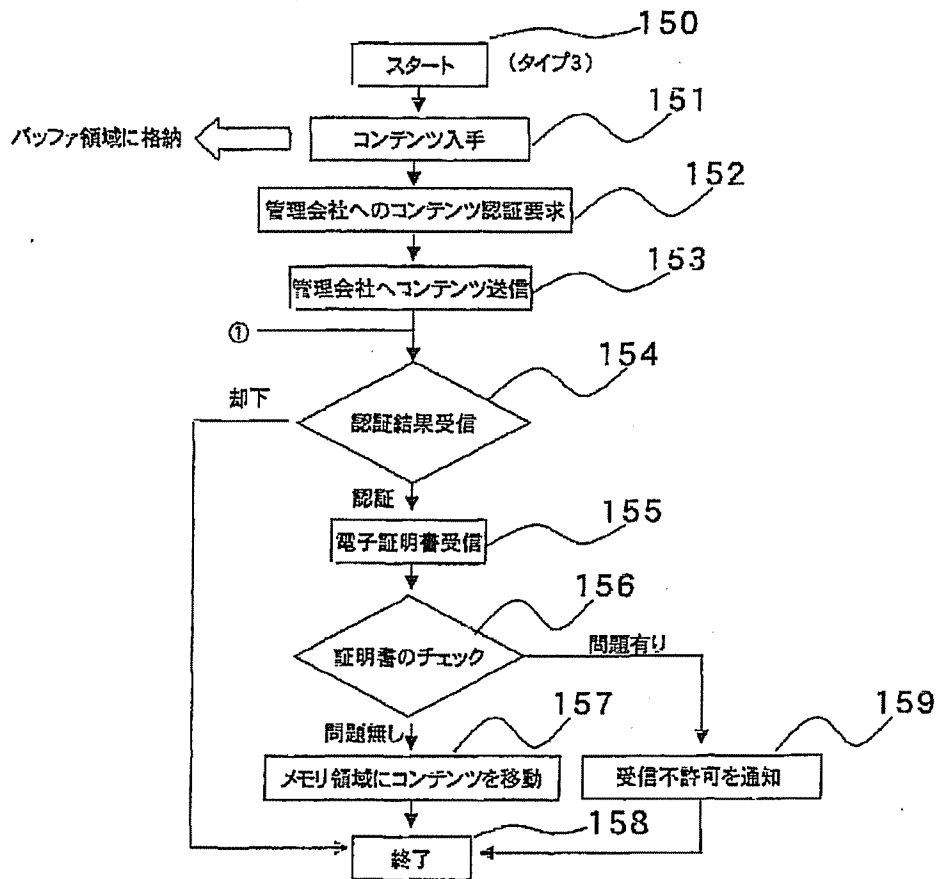


図 12

【図13】

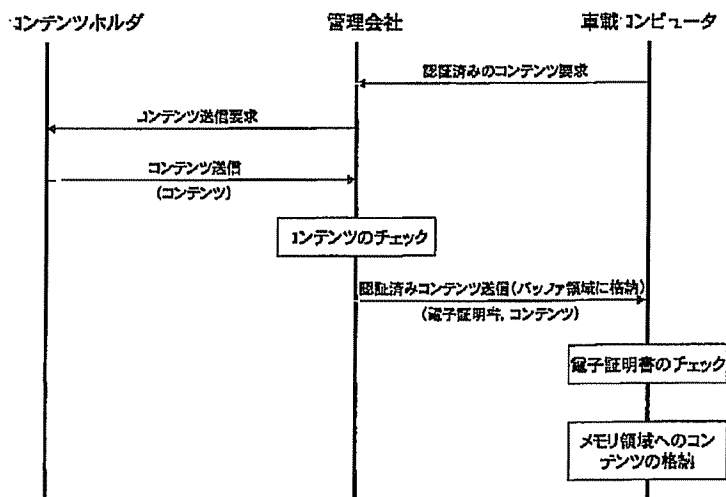


図 13

【図14】

